REMARKS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1, 4-9, 12-16, 19, 22-26, 29-33, 36, 39-43, 46 and 179-180 are presently active in this case. Claims 2-3, 10-11, 17-18, 20-21, 27-28, 34-35, 37-38, 44-45, and 47-178 were cancelled by previous Amendments. The present Amendment amends Claims 1, 5, 13, 15-16, 19, 23, 30, 32-33, 36, 40 and 46; and adds new Claims 179-182 without introducing any new matter.

The outstanding Office Action rejected Claims 1, 4, 7, 12, 16, 19, 22, 24, 29, 33, 36, 39, 41, 46 under 35 U.S.C. §102(e) as being anticipated by Ginter et al. (U.S. Patent No. 6,253,193, hereinafter "Ginter"). Claims 5-6, 23, and 40 were rejected under 35 U.S.C. §103(a) as unpatentable over Ginter in view of Teppler et al. (Patent No. 6,898,709 hereinafter "Teppler"). Claims 8, 25 and 42 were rejected under 35 U.S.C. §103(a) as unpatentable over Ginter in view of Orrin (Patent No. 6,011,849). Claims 9, 26 and 43 were rejected under 35 U.S.C. §103(a) as unpatentable over Ginter in view of Orrin and further in view of Kuroda. Claims 13-15 and 30-32 were rejected under 35 U.S.C. §103(a) as unpatentable over Ginter in view of Bodo (Patent No. 5,680,587).

In response, independent Claims 1, 19, 36 and 46 are amended to clarify certain features. In particular, independent Claim 1 is amended to clarify features regarding the generation

of the first and second integrity check values. Claim 1, as amended, now recites *inter alia*, a cryptography process section configured to split a first portion of header data of the content data having data on usage policy into a plurality of first messages, ***generate a first integrity check value or values to verify integrity of the header data by using said plurality of first messages***, split a second portion of the header data of the content data having a content key into a plurality of second messages, ***generate a second integrity check value or values*** to verify integrity of the header data by using said plurality of second messages, and ***generate an intermediate integrity check value based on said first integrity check value or values and said second integrity check value or values***. Dependent Claims 5, 13, and 15-16 are amended to correspond to the changes made in independent Claim 1.

These features find non-limiting support in applicants' disclosure as originally filed, with reference to Figures 4-7 and 22-23 and with the corresponding passages in the specification. For example page 26, paragraph [0396], lines 1-7, explaining in a non-limiting embodiment the data structures of the content data, recites that "[t]he configuration shown in FIG. 4 shows the format of the entire content data, the configuration shown in FIG. 5 shows details of the 'usage policy' partly constituting the header section of the content data, and the configuration shown in FIG. 6 shows details of the

'block information table' partly constituting the header section of the content."

In addition, applicants' specification explains in a non-limiting example that information of the user policy is used to calculate an integrity check value, see for example at page 35, paragraph [0541], lines 6-13, where it is explained with reference to Figures 7 and 23 that "[t]he integrity check value A is calculated in accordance with the ICV calculation method described in FIG. 7, using as a key the integrity-check-value-A-generating key Kicva stored in the internal memory 307 of the recording and reproducing device cryptography process section 302 and using the content ID and the usage policy as a message, as shown in FIG. 23." Applicants' Figure 23 further explains that messages M1 to MN are from the content ID and the usage policy, providing non-limiting support for header data being split into messages. In addition, page 35, paragraph [0542], lines 1-3, recite that "[a]s previously described in FIG. 4, the check value A, ICVa is used to verify that the content ID and the usage policy have not been tampered."

Applicants' specification also explains in a non-exhaustive example that data on usage policy may include "constituent information of content data, for example, the sizes of a header section and a content section constituting the content data, a format version, a content type indicating whether the content is a program or data, a localization field

indicating whether the content can be used only in an apparatus that has downloaded the content or also in other apparatuses," as explained in reference to page 25, paragraph [0379].

Regarding the features of generating second integrity check values, applicants' disclosure as originally filed also supports these features with non-limiting embodiment, for example at page 36, paragraph [0548], lines 1-4. This passage recites "[a]s previously described in FIG. 4, the check value B, ICVb is used to verify that the block information table key Kbit, the content key Kcon, and the block information table (BIT) have not been tampered."

In view of the above, it is believed that the amendments to independent Claim 1 find non-limiting support in the specification as originally filed, and therefore do not constitute new matter.

New claims are also added for examination. New Claims 179 and 181 depend upon Claims 1 and 19, respectively, and recite "wherein the plurality of messages provide multiple input data for a staged encryption." New Claims 179 and 181 find non-limiting support in applicants' disclosure with reference to Figures 7 and 23, and at page 27, paragraph [0423], lines 1-8, explaining that "[a] method for generating an electronic signature using a general DES will be explained with reference to FIG. 7. First, before generating an electronic signature, a message to which the electronic signature is to be added is

divided into sets of 8 bytes (the pieces of the divided message are hereafter referred to as "M1, M2, … , MN")."

New Claims 180 and 182 depend upon Claims 1 and 19, respectively, and recite "the first and second integrity check values are added to the header of the content data." New Claim 180 and 182 find non-limiting support in the last lines of page 35, paragraph [0541] of applicants' specification where it states "finally, the integrity check value A and the check value: ICVa stored in the header are compared together, and if they are equal, the process proceeds to step S53."

Turning now to the applied references, Ginter appear to describe a system for secure transaction and management of electronic rights (See Ginter in the Title and the Abstract). For this purpose, Ginter uses a VDE 100 that is defined as being a virtual distribution environment, able to handle and control electronic stored information (Abstract, column 4, lines 47-56), such as VDE objects 300 (FIG. 12a).

However, the portions of Ginter relied on by the outstanding Office Action fail to teach or suggest the steps of generating the first and second integrity check values, as required by applicants' claim 1, as next explained.

The outstanding Office Action merely points to different passages of Ginter, where different types of permission access and verification manipulation are shown, in a virtual distribution environment VDE 100. For example, the

outstanding Office Action points to method 1000. However, method 1000 is defined by Ginter as being "[a] 'method' 1000 provided by the preferred embodiment is a collection of basic instructions and information related to the basic instructions, that provides context, data, requirements and/or relationships for use in performing, and/or preparing to perform, the basic instructions in relation to the operation of one or more electronic appliances 600" (in Ginter at column 136, lines 20-51). Furthermore, Ginter shows different types of data structures that can be found in the private header 804 (column 137, lines 65-67).

Ginter then explains that "[w]hen encrypted or otherwise secured information is delivered into a user's secure VDE processing area (e.g., PPE 650), a portion of this information can be used as a "tag" that is first decrypted or otherwise unsecured and then compared to an expected value to confirm that the information represents expected information." (column 217, lines 13-20), and in this respect recites that "[v]alidation tags may be used to help detect record substitution attempts on the part of a tampered."

In light of the above passages, the outstanding Office Action asserts that the teachings of Ginter reciting and "overall check value" in Figure 26a, reference numeral 980, and at column 153, lines 8-10, is equivalent to "the intermediate integrity check value" of applicants' Claim 1. Assuming

arguendo that an overall check value is a result of an overall check, but the applied portions of Ginter fail to recite the features of Claim 1 regarding the generation of the first and second integrity check values. In addition, regarding Ginter's overall check value field 980, Ginter merely recites in this passage that "[i]n this example of PERC 808 also includes one or more rights records 906, and an overall check value field 980." No other information is given regarding the overall check value field.

Accordingly, the cited passages of Ginter clearly fail to teach all the Claim 1 features. For example, such portions of Ginter fail to teach "a cryptography process section configured to split a first portion of header data of the content data having data on usage policy into a plurality of first messages, generate a first integrity check value or values to verify integrity of the header data by using said plurality of first messages."

The cited passages of the remaining references Teppler, Orrin, Kipoda and Bodo also fail to teach the above identified features of applicants' Claim 1. Accordingly, even if we assume that the combination of these references were proper, the rejections under 35 U.S.C. §103(a) are also believed to be overcome.

Independent Claims 19, 36 and 46 recite features similar to or somewhat similar to the features recited in

independent Claim 1. Moreover, Claims 19, 36 and 46 have been amended in a manner similar to the amendment to Claim 1. Accordingly, for reasons similar to that stated above for the patentability of Claim 1, applicants respectfully submit that the rejections of Claims 19, 36 and 46, and the rejection of all associated dependent claims, are also believed to be overcome in view of the arguments regarding independent Claim 1.

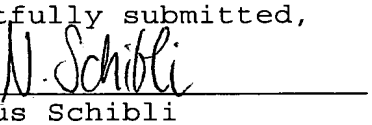
As it is believed that all of the rejections set forth in the Official Action have been fully met, favorable reconsideration and allowance are earnestly solicited.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he/she telephone applicant's representative at (908) 654-5000 in order to overcome any additional objections which he might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: December 22, 2006

Respectfully submitted,

By 

Nikolaus Schibli
Patent Agent
Registration No.: 56,994
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000

Attorney for Applicant

715461_1.DOC